

# Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/US05/006909

International filing date: 03 March 2005 (03.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: US  
Number: 60/554,687  
Filing date: 19 March 2004 (19.03.2004)

Date of receipt at the International Bureau: 18 April 2005 (18.04.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland  
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

1305811

# THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

*April 07, 2005*

**THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE.**

**APPLICATION NUMBER: 60/554,687**

**FILING DATE: *March 19, 2004***

**RELATED PCT APPLICATION NUMBER: *PCT/US05/06909***



Certified by

Under Secretary of Commerce  
for Intellectual Property  
and Director of the United States  
Patent and Trademark Office

17175 U.S. PTO  
031904

PTO/SB/16 (01-04)

Approved for use through 07/31/2006. OMB 0651-0032

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**PROVISIONAL APPLICATION FOR PATENT COVER SHEET**

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

Express Mail Label No. **EV406600057 US**

| INVENTOR(S)  |  |                        |  |   |  |
|--|--|------------------------|--|---|--|
| Given Name (first and middle [if any])   |  | Family Name or Surname |  | Residence<br>(City and either State or Foreign Country) |  |
| Harry  |  | VIG                    |  | Billerica, MA   |  |
| Additional inventors are being named on the _____ separately numbered sheets attached hereto   |  |                        |  |   |  |
| TITLE OF THE INVENTION (500 characters max)<br><b>LASER AUTO-CALIBRATION for QKD SYSTEMS</b>   |  |                        |  |   |  |
| Direct all correspondence to: CORRESPONDENCE ADDRESS   |  |                        |  |   |  |
| <input checked="" type="checkbox"/> Customer Number: <b>36522</b>  |  |                        |  |   |  |
| OR   |  |                        |  |   |  |
| <input type="checkbox"/> Firm or Individual Name   |  |                        |  |   |  |
| Address  |  |                        |  |   |  |
| Address  |  |                        |  |   |  |
| City   |  | State                  |  | Zip   |  |
| Country  |  | Telephone              |  | Fax   |  |
| ENCLOSED APPLICATION PARTS (check all that apply)  |  |                        |  |   |  |
| <input checked="" type="checkbox"/> Specification Number of Pages <b>17</b>  |  |                        |  |   |  |
| <input type="checkbox"/> CD(s), Number _____   |  |                        |  |   |  |
| <input checked="" type="checkbox"/> Drawing(s) Number of Sheets <b>3</b>   |  |                        |  |   |  |
| <input checked="" type="checkbox"/> Other (specify) <b>return receipt postcard</b>   |  |                        |  |   |  |
| <input type="checkbox"/> Application Data Sheet. See 37 CFR 1.76   |  |                        |  |   |  |
| METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT   |  |                        |  |   |  |
| <input checked="" type="checkbox"/> Applicant claims small entity status. See 37 CFR 1.27.   |  |                        |  |   |  |
| <input type="checkbox"/> A check or money order is enclosed to cover the filing fees.  |  |                        |  |   |  |
| <input checked="" type="checkbox"/> The Director is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number: <b>502992</b> |  |                        |  |   |  |
| <input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.  |  |                        |  |   |  |
| FILING FEE Amount (\$)<br><b>\$80</b>  |  |                        |  |   |  |
| The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.                        |  |                        |  |   |  |
| <input checked="" type="checkbox"/> No.  |  |                        |  |   |  |
| <input type="checkbox"/> Yes, the name of the U.S. Government agency and the Government contract number are: _____   |  |                        |  |   |  |

[Page 1 of 2]

Respectfully submitted,

SIGNATURE

*Joseph E. Gortych*

TYPED or PRINTED NAME

**Joseph E. Gortych**

TELEPHONE

**802-655-7222**

Date

**March 18, 2004**

REGISTRATION NO.

**41,791**

(if appropriate)

Docket Number:

**060-03P**

**USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT**

This collection of information is required by 37 CFR 1.51. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop Provisional Application, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

17175  
U.S. PTO  
031904

PTO/SB/17 (10-03)

Approved for use through 07/31/2006. OMB 0651-0032  
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

# FEE TRANSMITTAL for FY 2004

Effective 10/01/2003. Patent fees are subject to annual revision.

☒ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT

(\$)  
80-

## Complete if Known

Application Number

Filing Date

March 19, 2004

First Named Inventor

VIG

Examiner Name

-

Art Unit

-

Attorney Docket No.

060-03P

## METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☒ Deposit Account:

Deposit  
Account  
Number  
Deposit  
Account  
Name

502992

Magic Technologies, Inc.

The Director is authorized to: (check all that apply)

☒ Charge fee(s) indicated below ☒ Credit any overpayments

☒ Charge any additional fee(s) or any underpayment of fee(s)

☐ Charge fee(s) indicated below, except for the filing fee to the above-identified deposit account.

## FEE CALCULATION

### 1. BASIC FILING FEE

Large Entity Small Entity

| Fee Code     | Fee (\$) | Fee Code | Fee (\$) | Fee Description        | Fee Paid    |
|--------------|----------|----------|----------|------------------------|-------------|
| 1001         | 770      | 2001     | 385      | Utility filing fee     |             |
| 1002         | 340      | 2002     | 170      | Design filing fee      |             |
| 1003         | 530      | 2003     | 265      | Plant filing fee       |             |
| 1004         | 770      | 2004     | 385      | Reissue filing fee     |             |
| 1005         | 160      | 2005     | 80       | Provisional filing fee | 80          |
| SUBTOTAL (1) |          |          |          |                        | (\$)<br>80- |

### 2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

| Total Claims       | Extra Claims | Fee from below | Fee Paid |
|--------------------|--------------|----------------|----------|
| Independent Claims | -20** =      | X              |          |
| Multiple Dependent | -3** =       | X              |          |

| Large Entity | Small Entity | Fee Description  |
|--------------|--------------|--|
| Fee Code     | Fee Code     | Fee (\$)   |
| 1202         | 2202         | 9 Claims in excess of 20                                     |
| 1201         | 2201         | 43 Independent claims in excess of 3                         |
| 1203         | 2203         | 145 Multiple dependent claim, if not paid                    |
| 1204         | 2204         | 43 ** Reissue independent claims over original patent        |
| 1205         | 2205         | 9 ** Reissue claims in excess of 20 and over original patent |
| SUBTOTAL (2) |              |  |

\*\*or number previously paid, if greater; For Reissues, see above

## FEE CALCULATION (continued)

### 3. ADDITIONAL FEES

Large Entity Small Entity

| Fee Code | Fee (\$) | Fee Code | Fee (\$) | Fee Description  | Fee Paid |
|----------|----------|----------|----------|--|----------|
| 1051     | 130      | 2051     | 65       | Surcharge - late filing fee or oath  |          |
| 1052     | 50       | 2052     | 25       | Surcharge - late provisional filing fee or cover sheet                     |          |
| 1053     | 130      | 1053     | 130      | Non-English specification  |          |
| 1812     | 2,520    | 1812     | 2,520    | For filing a request for ex parte reexamination                            |          |
| 1804     | 920*     | 1804     | 920*     | Requesting publication of SIR prior to Examiner action                     |          |
| 1805     | 1,840*   | 1805     | 1,840*   | Requesting publication of SIR after Examiner action                        |          |
| 1251     | 110      | 2251     | 55       | Extension for reply within first month                                     |          |
| 1252     | 420      | 2252     | 210      | Extension for reply within second month                                    |          |
| 1253     | 950      | 2253     | 475      | Extension for reply within third month                                     |          |
| 1254     | 1,480    | 2254     | 740      | Extension for reply within fourth month                                    |          |
| 1255     | 2,010    | 2255     | 1,005    | Extension for reply within fifth month                                     |          |
| 1401     | 330      | 2401     | 165      | Notice of Appeal   |          |
| 1402     | 330      | 2402     | 165      | Filing a brief in support of an appeal                                     |          |
| 1403     | 290      | 2403     | 145      | Request for oral hearing   |          |
| 1451     | 1,510    | 1451     | 1,510    | Petition to institute a public use proceeding                              |          |
| 1452     | 110      | 2452     | 55       | Petition to revive - unavoidable   |          |
| 1453     | 1,330    | 2453     | 665      | Petition to revive - unintentional   |          |
| 1501     | 1,330    | 2501     | 665      | Utility issue fee (or reissue)   |          |
| 1502     | 480      | 2502     | 240      | Design issue fee   |          |
| 1503     | 640      | 2503     | 320      | Plant issue fee  |          |
| 1460     | 130      | 1460     | 130      | Petitions to the Commissioner  |          |
| 1807     | 50       | 1807     | 50       | Processing fee under 37 CFR 1.17(q)  |          |
| 1806     | 180      | 1806     | 180      | Submission of Information Disclosure Stmt                                  |          |
| 8021     | 40       | 8021     | 40       | Recording each patent assignment per property (times number of properties) |          |
| 1809     | 770      | 2809     | 385      | Filing a submission after final rejection (37 CFR 1.129(a))                |          |
| 1810     | 770      | 2810     | 385      | For each additional invention to be examined (37 CFR 1.129(b))             |          |
| 1801     | 770      | 2801     | 385      | Request for Continued Examination (RCE)                                    |          |
| 1802     | 900      | 1802     | 900      | Request for expedited examination of a design application                  |          |

Other fee (specify)

\*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) (\$)  
0

## SUBMITTED BY

Name (Print/Type) Joseph E. Gortuch  
Signature [Signature]

Registration No. 41,791  
(Attorney/Agent)

(Complete if applicable)

Telephone 802 655 7222  
Date 03/18/04

**WARNING:** Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

This collection of information is required by 37 CFR 1.17 and 1.27. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

## **LASER AUTOCALIBRATION FOR QKD SYSTEMS**

### **Field of the Invention**

5           The present invention relates to quantum cryptography, and in particular relates to apparatus and methods of autocalibrating the laser of a quantum key distribution (QKD) system to maintain optimal system performance.

### **Background of the Invention**

10           Quantum key distribution involves establishing a key between a sender ("Alice") and a receiver ("Bob") by using weak (e.g., 0.1 photon on average) optical signals ("photon signals") transmitted over a "quantum channel." The security of the key distribution is based on the quantum mechanical principal that any measurement of a quantum system in unknown state will modify its state. As  
15           a consequence, an eavesdropper ("Eve") that attempts to intercept or otherwise measure the photon signals will introduce errors into the transmitted signals, thereby revealing her presence.

          The general principles of quantum cryptography were first set forth by Bennett and Brassard in their article "Quantum Cryptography: Public key  
20           distribution and coin tossing," Proceedings of the International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984, pp. 175-179 (IEEE, New York, 1984). A specific QKD system is described in U.S. Patent No. 5,307,410 to Bennett (the '410 patent).

          The above-mentioned publications each describe a so-called "one-way"  
25           QKD system wherein Alice randomly encodes the polarization or phase of the photon signals, and Bob randomly measures the polarization or phase of the photon signals. The one-way system described in the Bennett 1992 paper is based on two optical fiber Mach-Zehnder interferometers. Respective parts of the interferometric system are accessible by Alice and Bob so that each can  
30           control the phase of the interferometer. The signals (pulses) sent from Alice to Bob are time-multiplexed and follow different paths. As a consequence, the

interferometers need to be actively stabilized to within a few tens of nanoseconds during transmission to compensate for thermal drifts.

U.S. Patent No. 6,438,234 to Gisin (the '234 patent), which patent is incorporated herein by reference, discloses a so-called "two-way" QKD system that is autocompensated for polarization and thermal variations. Thus, the two-way QKD system of the '234 patent is less susceptible to environmental effects than a one-way system.

When operating a commercial QKD system, multiple variables need to be aligned in time and then maintained aligned for optimal system performance. For example, in a commercial QKD system one or more single-photon detectors are gated with a gating signal from a controller to synchronize the detection of optical pulses with expected pulse arrival times. However, once the system is set up, the timing drifts due to various systemic and environmental factors and the photon count can drop. This leads to a reduction in the transmission rate of the system, and also to an increase in the bit-error rate—i.e., to less than optimal system performance.

While laboratory and prototype QKD systems can be adjusted to account for system drifts under very controlled and artificial conditions, making the necessary adjustments for a commercial QKD system in the field is a far more daunting endeavor. And, unlike with a laboratory or prototype QKD system, end-users of commercial QKD systems have an expectation that their QKD system will automatically run in an optimal state with minimal or no operator intervention.

### **Summary of the Invention**

A first aspect of the invention is a method of autocalibrating a QKD system having two encoding stations, where one of the encoding stations includes a laser and a controller. The method includes performing a laser gate scan by sending a laser gating signals from the controller to the laser and varying the arrival time  $T$  of the signal over a first select range  $R1$ . The method also includes determining an optimal timing  $T_{MAX}$  for the laser gate signal that corresponds to a maximum number of photon counts  $N_{MAX}$  from the single-photon detector (SPD) unit when exchanging photon signals between encoding stations of the QKD

system. The method further includes performing laser gate signal dithering by varying the arrival time  $T$  over a second select range  $R2$  surrounding  $T_{MAX}$  to maintain the photon count at a maximum value.

A second aspect of the invention is method of exchanging a key in a quantum key distribution (QKD) system having two encoding stations, and a laser coupled to a controller in one of the encoding stations. The method includes using a laser to generate photon signals and exchanging the photon signals between the encoding stations in the QKD system. The method also includes performing a first laser gate scan. The first laser gate scan is accomplished by sending laser gating signals from the controller to the laser over a range of laser gating signal arrival times  $T$  to establish a first optimal arrival time  $T_{MAX}$  for the laser gate signal corresponding to a first maximum number of photon counts  $N_{MAX}$  from the detector. The method also includes terminating the first laser gate scan when the first  $T_{MAX}$  is established, and then performing a first laser gate dither. The first laser gate dither is accomplished by the controller altering the arrival time  $T$  of the (optimum) laser gate signal over a range of arrival times  $R2$  about the first  $T_{MAX}$  to maintain either the maximum number of photon counts  $N_{MAX}$  or a different maximum number of photon counts  $N'_{MAX}$  over the range  $R2$ .

A third aspect of the invention is a continuation of the method of the second aspect of the invention, wherein performing the laser gate dither results in a new optimal arrival time  $T'_{MAX}$ . The method of the third aspect of the invention includes terminating the performing of a laser gate dither, performing a second laser gate scan, terminating the second laser gate scan, and then performing a second laser gate dither to automatically reestablish optimal system performance.

### **Brief Description of the Drawings**

FIG. 1 is an example embodiment of a two-way QKD system suitable for implementing the method of the present invention;

FIG. 2 is a flow diagram illustrating the laser autocalibration method, which includes scanning and dithering of the laser gate signal to optimize the photon count while exchanging photon signals; and

FIG. 3 is an example plot of a single-photon laser gate scan for a QKD system such as that shown in FIG. 1, wherein the Y-axis is the number of photon counts  $N$  in a regular time interval from the SPD unit, and the X-axis is the timing (arrival time) of the laser gate signal.

The various elements depicted in the drawings are merely representational and are not necessarily drawn to scale. Certain sections thereof may be exaggerated, while others may be minimized. The drawings are intended to illustrate various embodiments of the invention that can be understood and appropriately carried out by those of ordinary skill in the art.

### **Detailed Description of the Invention**

The present invention relates to methods of performing autocalibration of the laser in a QKD system to maintain optimal system performance. In particular, the present invention involves performing laser gate signal scanning to determine the optimal laser gate signal position (timing), as well as performing laser gate signal timing dithering in order to maintain the optimal laser gate signal size (i.e., width) and position during the QKD system's operation. This results in optimal photon signal detection (i.e., the greatest number of photon signal counts) in the QKD system, which generally corresponds to the optimal operation of the QKD system as a whole.

The invention is applicable to one-way, two-way and ring topology or  $n$ -way QKD systems using either polarization encoding or phase encoding, and using one or more single-photon detectors. The invention is described below in connection with an example embodiment of a two-way QKD system using phase-encoding and a single-photon detector unit having two detectors. This choice of QKD system is merely for the sake of illustrating the methods of the present invention, and is no way intended as limiting.

Also, in the description below, a "gate signal" is a signal that activates the element to which the signal is sent, wherein the activation of the element

corresponds to the duration (width  $W$ ) of the signal. Thus, the laser gate signal activates the laser for the duration (i.e., width) of the laser gate signal, wherein activation starts at the leading edge of the pulse and ends at the trailing edge of the pulse. In the case of the pulsed laser, the optical pulse is emitted from the laser at some point during the width of the laser gate signal (say, at the rising edge of the gate signal), and the resulting optical pulse may have an optical pulse width smaller than that of the width of the laser gate signal.

Also, in the discussion below, the laser generates optical pulses used to exchange keys between the two encoding stations of the QKD system. In a preferred embodiment, these pulses are attenuated after they leave the laser to form the quantum pulses (referred to below as "photon signals") that have, on average, one photon or less. Thus, in the description below and in the claims, the phrase "photons signals generated by the laser" and similar phrases are understood to include the case where the laser generates relatively strong optical pulses that are later attenuated (e.g., via a variable attenuator) to form the photon signals.

### ***QKD system embodiment***

FIG. 1 is a schematic diagram of an example embodiment of a folded QKD system 200 to which the methods of the present invention are aptly suited. System 200 includes two key encoding ("encoding") stations: a transmitting/receiving station Bob and a reflecting station Alice, referred to hereinafter simply as "Bob" and "Alice."

#### **Bob**

With continuing reference to FIG. 1, Bob includes a laser 202 that emits optical pulses 204. In an example embodiment, laser 202 is a laser diode and includes a back facet monitor (BFM) 203. Laser 202 is coupled to a time-multiplexing/demultiplexing optical system 206 having an input end 208A, an input/output end 208B, and a detector output end 208C. Optical system 206 receives input pulses 204 at input end 208A, splits each pulse into two time-multiplexed pulses P1 and P2 and outputs them at input/output end 208B.

Likewise, optical system 206 also receives optical pulses at input/output end 208B, as described below.

A single-photon detector (SPD) unit 216 is coupled to optical system 206 at detector output end 208C. In an example embodiment, SPD unit 216 includes two SPDs 216A and 216B. A phase modulator (PM) 220 is coupled (e.g., by an optical fiber) to optical system input/output end 208B. An optical fiber 240 connects Bob to Alice at PM 220.

Bob also includes a controller 248 operatively (e.g., electrically) coupled to laser 202, BFM 203, SPD unit 216, and PM 220 to control the operation of these elements, as described below. In an example embodiment, controller 248 includes a programmable computer capable of performing instructions (e.g., "software") stored on a computer-readable medium 250. In an example embodiment, the instructions stored on the computer-readable medium 250 include methods according to the present invention as described below.

#### Alice

Alice includes a variable optical attenuator (VOA) 264 connected to optical fiber 240. A phase modulator (PM) 266 is arranged downstream of and is optically coupled to VOA 264. A Faraday mirror 270 is arranged downstream of and is optically coupled to PM 266.

Alice also includes a controller 288 operatively (e.g., electrically) coupled to PM 266 and VOA 264. In an example embodiment, controller 288 includes a programmable computer capable of performing instructions (e.g., "software") stored on a computer-readable medium 289. In an example embodiment, the instructions stored on the computer-readable medium 289 include methods according to the present invention as described below.

Controllers 248 and 288 are linked (e.g., electrically or optically) via link 290 to synchronize the operation of Alice and Bob. In particular, the operation of the laser 202, phase modulators 220 and 266, and SPD unit 216 are controlled and coordinated by controllers 248 and 288 relative to the launched optical pulse 204 using gating signals S0, S2, S3 and S1, respectively, when exchanging a quantum key between Alice and Bob. Thus, in an example embodiment,

controllers 248 and 288 can be considered as constituting a single controller for the QKD system.

### ***QKD System Operation***

5           With continuing reference to FIG. 1, in the operation of system 200, a laser gating signal S0 is sent by controller 248 to laser 202 to generate optical pulse 204. Optical pulse 204 is then divided into two separate pulses P1 and P2 by time-multiplexing/demultiplexing optical system 206. In an example embodiment, pulses P1 and P2 are relatively weak pulses, but can be strong  
10           pulses attenuated later at Alice prior to returning to Bob to form photon signals. The optical pulses P1 and P2 are passed out of optical system input/output end 208B to PM 220, which is gated to allow the pulses to pass therethrough unmodulated. Pulses P1 and P2 then pass to Alice over optical fiber 240. Pulses P1 and P2 continue to VOA 264, which can attenuate the pulses if  
15           necessary. The pulses then pass through PM 266 and are reflected by Faraday mirror 270, and then pass back through PM 266 a second time.

          During one of the passes of pulses P1 and P2 through PM 266, the PM modulates one of the pulses -- say, pulse P1 -- to form a phase-modulated pulse P1'. This is achieved by controller 288 sending a well-timed gating signal S1 that  
20           activates PM 266 for the short period of time (i.e., less than the time-separation between the pulses) when pulse P1 passes through PM 266. Pulses P1 and P2 then pass back through VOA 264, which can attenuate the pulses, if necessary, to ensure that photon signals (i.e., optical pulses having an average number of photons of one or less) are exchanged between Bob and Alice.

25           The pulses then pass back to Bob as photon signals and pass to PM 220 therein. PM 220 is then directed to randomly modulate one of the pulses -- say the remaining unmodulated pulse P2 -- with one of the select phase modulation values. This is achieved by controller 248 providing a well-time gating signal S2 to PM 220 that activates the phase modulator during the short time period within  
30           which pulse P2 passes through PM 220.

          Now-modulated pulses P1' and P2' (the latter is not shown in FIG. 1) continue on to optical system 206. Optical system 206 combines the pulses to

form a combined pulse P3, which is directed out of detector output end 208C to SPD unit 216. SPD unit 216 receives combined pulse P3 and outputs a signal to controller 248 that corresponds to the relative phases imparted to pulses P1 and P2 by PM's 266 and 206, respectively. In an example embodiment, one of  
5 detectors 216A and 216B receives the interfered pulse P3, depending on whether the interference is constructive or destructive.

Once a desired number of photon signals are exchanged, the key is derived using prior art techniques—for example, by Alice and Bob publicly comparing the basis of their measurements and only keeping the measurements  
10 (bits) corresponding to the same measurement basis. This forms the sifted key. They then choose a subset of the remaining bits to test for the presence of an eavesdropper Eve and then discard these bits. The act of eavesdropping on optical fiber 240 by Eve intercepting or otherwise attempting to measure the weak optical pulses being transmitted between Bob and Alice will necessarily  
15 introduce errors in the key due to the quantum nature of the photons being exchanged. If there are no errors in the sifted key due to the presence of an eavesdropper Eve, then the transmission is considered secure, and the quantum key is established.

## 20 ***Methods of Maintaining Optimal System Operation***

FIG. 2 is a flow diagram 300 of the method of the present invention for maintaining optimal system operation of QKD system 200. The method involves performing both a laser gate scan and a laser gate dither in the manner described below.

25 In 302, the key exchange process is initiated by controller 248 sending laser gate signal S0 to laser 202 to emit optical pulses 204 so that time-multiplexed optical pulses P1 and P2 can be sent from Bob to Alice. This process includes controller 288 instructing PM 266 via gating signal S1 to phase modulate one of the pulses, having the pulses travel back to Bob, modulating the  
30 remaining pulse, combining the modulated pulses, and detecting the combined pulse P3 in SPD unit 216, as described above.

In 304, a laser gate scan is performed. This involves varying the timing (e.g., the arrival time  $T$ ) of laser gate signal  $S0$  over a selected range  $R1$  of timing values to establish the optimal gate timing (arrival time)  $T_{MAX}$  that yields the maximum number of photon counts  $N_{MAX}$  of exchanged photon signals detected by SPD unit 216.

It is worth noting that in the case where SPD unit 216 includes two detectors 216A and 216B, it is typically a good presumption that drifts (e.g., thermal drifts) occurring in the SPD unit affect SPDs 216A and 216B to essentially the same extent, so that the two SPD drift together.

In an example embodiment of the laser gate scan, the width  $W$  of laser gate signal  $S0$  is also optionally varied over a selected pulse width range  $RW1$  to establish the optimum laser gate signal width  $W_{MAX}$ .

FIG. 3 is an example plot of the results of a laser gate scan, wherein the Y-axis is the number  $N$  of photon counts obtained by SPD unit 216 associated with a given laser gate scan time  $T$ . The X-axis represents the relative timing (e.g., arrival time  $T$ ) of the laser gate signal  $S0$ , which is varied to achieve maximum number of photon counts  $N_{MAX}$ . In the context of the present invention, the maximum number of photon counts  $N_{MAX}$  corresponds to optimal system performance because it corresponds to the highest data transmission rates and highest photon signal sensitivity level vs. timing, with no increase in dark current counts. Likewise, in an example embodiment of the present invention, an optimal photon signal is one that optimizes the ratio of photon pulses to dark event pulses, while maintaining a smooth detector response that allows for laser gate dithering, as described below.

The curve in FIG. 3 is obtained by incrementing the arrival time  $T$  of the laser gate signal  $S0$  over a select range  $R1$  of timing values  $T$  (X-axis). In an example embodiment, the arrival time  $T$  corresponds to the position of the leading edge of the laser gate signal relative to a reference, e.g., a clock reference time provided by controller 248.

Once  $T_{MAX}$  and  $N_{MAX}$  are determined, then the process proceeds to 306, wherein the laser gate scan is terminated (i.e. is turned OFF).

In 308, laser gate dithering is performed. This involves repeatedly changing the timing (e.g., arrival time  $T$ ) and/or pulse width  $W$  of the laser gate signal  $S_0$  by small amounts within a select timing range  $R_2$  around the maximum (optimum) arrival time  $T_{MAX}$  (i.e., the laser gate signal is “dithered”). If necessary, the arrival time  $T$  is shifted from its original optimal value  $T_{MAX}$  to a new optimal value  $T'_{MAX}$  so that the photon count  $N$  is maintained at the maximum value  $N_{MAX}$  (or alternatively, to a new maximum photon count  $N'_{MAX}$ ). Note that select range  $R_2$  is less than  $R_1$  and is selected to surround a relatively small range about  $T_{MAX}$ . Also note that for optional laser gate width dithering, the laser gate signal width is dithered over a small range  $R_{W2}$  about the optimal pulse with  $W_{MAX}$ .

In an example embodiment, the timing range  $R_2$  is selected to be small enough to keep a security attacker (e.g., Eve) from leading the timing off to an undesirable location, yet large enough to allow for the dithering process to be successful, i.e., keep the photon count  $N$  at a maximum value  $N_{MAX}$ .

With reference again to FIG. 3, four data points  $d_1$ ,  $d_2$ ,  $d_3$  and  $d_4$  on the curve are highlighted for the sake of illustration. Assume the data point  $d_1$  is measured first, then the data point  $d_2$  associated with a greater arrival time  $T$  is measured. Since the number of photon counts associated with  $d_2$  is less than that associated with  $d_1$ , the arrival time  $T$  of the laser gate signal  $S_0$  is decreased. The number of photon counts for the laser gate signal position associated with data point  $d_1$  is re-measured. Since the number of photon counts  $N$  associated with the second data point at  $d_1$  is higher than that associated with data point  $d_2$ , the arrival time  $T$  is further decreased and the photons count is measured. The result is data point  $d_3$ , which has a higher photon count than for data point  $d_1$ . The arrival time  $T$  is thus decreased again, yield the lower photon count associated with a data point  $d_4$ . Since this measurement is less than that for  $d_3$ , the arrival time  $T$  of the laser gate signal  $S_0$  is increased, but not so much that it returns to the value associated with data point  $d_2$ .

In this manner, the laser gate signal timing is varied back and forth (“dithered”) until it converges on the maximum (or near-maximum) number of photon counts. Thus, during normal operation of SPD unit 216, the laser gate

dither process keeps the single-photon sensitivity high. In an example embodiment, laser gate dithering is performed periodically, for example every second. In an example embodiment, this rate is proportional to the number of single-photon counts received.

5           In 310, the choice of performing an autocalibration of the laser gate signal S0 by initiating another laser gate scan is presented. If such autocalibration is desired or otherwise deemed necessary, then the method proceeds to 312. In 312, the laser gate dither is turned OFF and the process returns to the laser gate scan of 304 to perform an updated calibration of the laser gate timing and/or  
10 laser gate signal width to find a new optimal arrival time  $T_{MAX}$  and/or optimal pulse width  $W_{MAX}$ . This updated calibration may need to be performed for a variety of reasons, such as a detected change in the environment or because of normal system drifts.

          In an example embodiment, autocalibration of the QKD system is  
15 performed when any of the following conditions occur: a) a change in photon count levels outside of statistical limits, b) ambient temperature changes greater than a predetermined amount such as 0.5°C occur, c) an optical path has changed configuration, as through a switching network element, different from event a), as in a message of a pending event will be sent before the change in  
20 photon count levels, d) on a daily schedule due to known daily temperature cycling, and e) on a fixed time basis, such as every hour, whether needed or not.

          The need to turn OFF the laser gate dither prior to performing the laser gate scan arises because the two processes can interfere with one another. Specifically, while the laser gate scan tries to increment the timing or width of the  
25 laser gate signal in a smooth (i.e., incremental) fashion, the laser gate dither tries to adjust the variable back and forth over small increments in order to stay on the maximum number of photon counts. Consequently, the two competing processes can produce spurious results. Thus, following a scan and update of the laser gate signal parameters during the laser gate scan of 304, the laser gate dither is  
30 automatically (or alternatively, is manually) turned back ON.

          If there is no desire or need to perform the autocalibration, then the method remains in the laser gate dither process of 308, which as mentioned

above is repeated, e.g., every second or so. The periodic laser gate dither process generally results in slight changes of the value of  $T_{MAX}$  in order to maintain the photon count at  $N_{MAX}$ , or alternatively to maintain the photon count at new maximum values  $N'_{MAX}$ ,  $N''_{MAX}$ , etc. For the sake of clarity and simplicity, in the present invention, "maximum photon counts" can mean  $N_{MAX}$  or  $N'_{MAX}$  or  $N''_{MAX}$ , etc. Likewise, the "optimal arrival time  $T_{MAX}$ " can change, and so in the present invention can mean  $T_{MAX}$ ,  $T'_{MAX}$  and  $T''_{MAX}$ , etc.

In an example embodiment, the above-described method of the present invention is embodied in at least one of computer readable medium 250 and 289 and is executed by at least one of controller 248 and 288 to carry out the method in QKD system 200.

In the foregoing Detailed Description, various features are grouped together in various example embodiments for ease of understanding. The many features and advantages of the present invention are apparent from the detailed specification, and, thus, it is intended by the appended claims to cover all such features and advantages of the described apparatus that follow the true spirit and scope of the invention. Furthermore, since numerous modifications and changes will readily occur to those of skill in the art, it is not desired to limit the invention to the exact construction, operation and example embodiments described herein.

Accordingly, other embodiments are within the scope of the appended claims.

What is claimed is:

1. A method of autocalibrating a quantum key distribution (QKD) system  
5 having two encoding stations, a laser and a single-photon detector (SPD) unit, comprising:
  - a) performing a laser gate scan by sending a laser gate signal to the laser and varying an arrival time  $T$  of the laser gate signal over a first select range  $R1$  to determine an optimal arrival time  $T_{MAX}$  that corresponds to a  
10 maximum number of counts  $N_{MAX}$  from the SPD unit for photon signals generated by the laser and exchanged between the two encoding stations; and
  - b) performing laser gate dithering by varying the arrival time  $T$  over a second select range  $R2$  surrounding  $T_{MAX}$  to maintain the photon count from the SPD unit at a maximum value.  
15
2. The method of claim 1, including:  
terminating the laser gate dithering and performing another laser gate scan.
- 20 3. The method of claim 1, wherein the QKD system includes a programmable controller and a computer readable medium, and wherein the method is embodied in the computer readable medium such that the controller is capable of directing the QKD system to carry out acts a) and b).
- 25 4. The method of claim 1, wherein performing the laser gate scan includes varying a laser gate signal width  $W$  over a range of pulse widths  $RW1$  to establish an optimal pulse width  $W_{MAX}$ .
5. The method of claim 4, wherein performing laser gate dithering includes  
30 varying the laser gate signal width  $W$  over a range of pulse widths  $RW2$  to maintain an optimal pulse width.

6. A computer-readable medium having instructions embodied therein to direct a computer in a quantum key distribution (QKD) system having a laser to perform the following method of autocalibrating the QKD system:

a) performing a laser gate scan by sending laser gate signals to the laser and varying an arrival time  $T$  of the laser gate signals over a first range  $R1$  to determine an optimal arrival time  $T_{MAX}$  that corresponds to a maximum number of photon counts  $N_{MAX}$  from an SPD unit; and

b) performing laser gate dithering by varying the arrival time  $T$  of the laser gate signals over a second select range  $R2$  surrounding  $T_{MAX}$  to maintain the number of photon counts from the SPD unit at a maximum value.

7. A method of exchanging a key in a quantum key distribution (QKD) system having a laser and an SPD unit both operably coupled to a controller, comprising:

exchanging photon signals between encoding stations in the QKD system, where the photon signals are generated by the laser;

performing a first laser gate scan by sending laser gate signals from the controller to the laser over a range of laser gate signal arrival times  $T$ ;

establishing from the first laser gate scan a first optimal arrival time  $T_{MAX}$  for the laser gate signal corresponding to a first maximum number of photon counts  $N_{MAX}$  from the detector;

terminating the first laser gate scan when the first  $T_{MAX}$  is established; and

performing a first laser gate dither by the controller altering the arrival time  $T$  over a range of arrival times  $R2$  about the first  $T_{MAX}$  to maintain either the maximum number of photon counts  $N_{MAX}$  or a different maximum number of photon counts  $N'_{MAX}$  over the range  $R2$ .

8. The method of claim 7, wherein performing the laser gate dither results in a new optimal arrival time  $T'_{MAX}$ .

9. The method of claim 7, further including:

terminating the performing of a laser gate dither; and

performing a second laser gate scan;  
terminating the second laser gate scan; and  
performing a second laser gate dither.

5 10. The method of claim 7, further including terminating and repeating the first laser gate dither periodically so as to perform a series of laser gate dithers.

11. A computer-readable medium having instructions embodied therein to direct a computer in a quantum key distribution (QKD) system to perform the following method of performing autocalibration of a single-photon detector arranged to detect photons in the QKD system:

sending photon signals between encoding stations in the QKD system, wherein the photon signals are generated by a laser coupled to a controller;

15 performing a first laser gate scan by sending laser gate signals from the controller to the detector over a range of laser gate signal arrival times  $T$  to establish a first optimal arrival time  $T_{MAX}$  corresponding to a first maximum number of photon counts  $N_{MAX}$  from the detector;

terminating the first laser gate scan when the first  $T_{MAX}$  is established; and

20 performing a first laser gate dither by the controller altering the arrival time  $T$  over a range of arrival times  $R2$  about the first  $T_{MAX}$  to maintain either the maximum number of photon counts  $N_{MAX}$  or a different maximum number of photon counts  $N'_{MAX}$  over the range  $R2$ .

12. A method of autocalibrating a single-photon detector in a quantum key distribution (QKD) system having a controller, comprising:

sending photon signals between encoding stations in the QKD system;

performing a first laser gate scan to determine an optimum arrival time of a laser gate signal sent from a controller to the detector;

terminating the first laser gate scan; and

30 periodically performing a laser gate dither to maintain a maximum number of photon counts from the detector.

12. The method of claim 11, further including:  
terminating the first laser gate dither; and  
performing a second laser gate scan;

5 13. A method of performing photon detector autocalibration in quantum key distribution (QKD) system having two encoding stations, and a laser coupled to a controller in one of the encoding stations, the method comprising:

performing a laser gate scan to establish an optimum arrival time of a laser gate signal that corresponds with a maximum number of photon counts from a single-photon detector (SPD) unit in one of the encoding stations when exchanging photon signals between the encoding stations;

terminating the laser gate scan; and

performing a laser gate dither process by varying the arrival time of the laser gate signal around the optimal value of the arrival time in order to provide minor adjustments to the arrival time of the laser gate signal that lead to the SPD unit yielding a maximum number of photon counts.

20

25

## LASER AUTOCALIBRATION FOR QKD SYSTEMS

### Abstract of the Invention

5

A method of performing autocalibration of the laser in a quantum key distribution (QKD) system (200) is disclosed. The method includes first performing a laser gate scan (304) to establish the optimum arrival time ( $T_{MAX}$ ) of a laser gate signal (S0) that corresponds with a maximum number of photon counts ( $N_{MAX}$ ) from a single-photon detector (SPD) unit (216) in the QKD system when exchanging photon signals between encoding stations (Alice and Bob) of the QKD system. Once the optimal laser gate signal arrival time (T) is determined, the laser gate scan is terminated and a laser gate dither process is initiated. The laser gate dither involves varying the arrival time of the laser gate  
10 signal around the optimal value of the arrival time  $T_{MAX}$  established during the laser gate scan process. The laser gate dither provides minor adjustments to the laser gate signal arrival time to ensure that the SPD unit produces maximum  
15 number of photon counts.

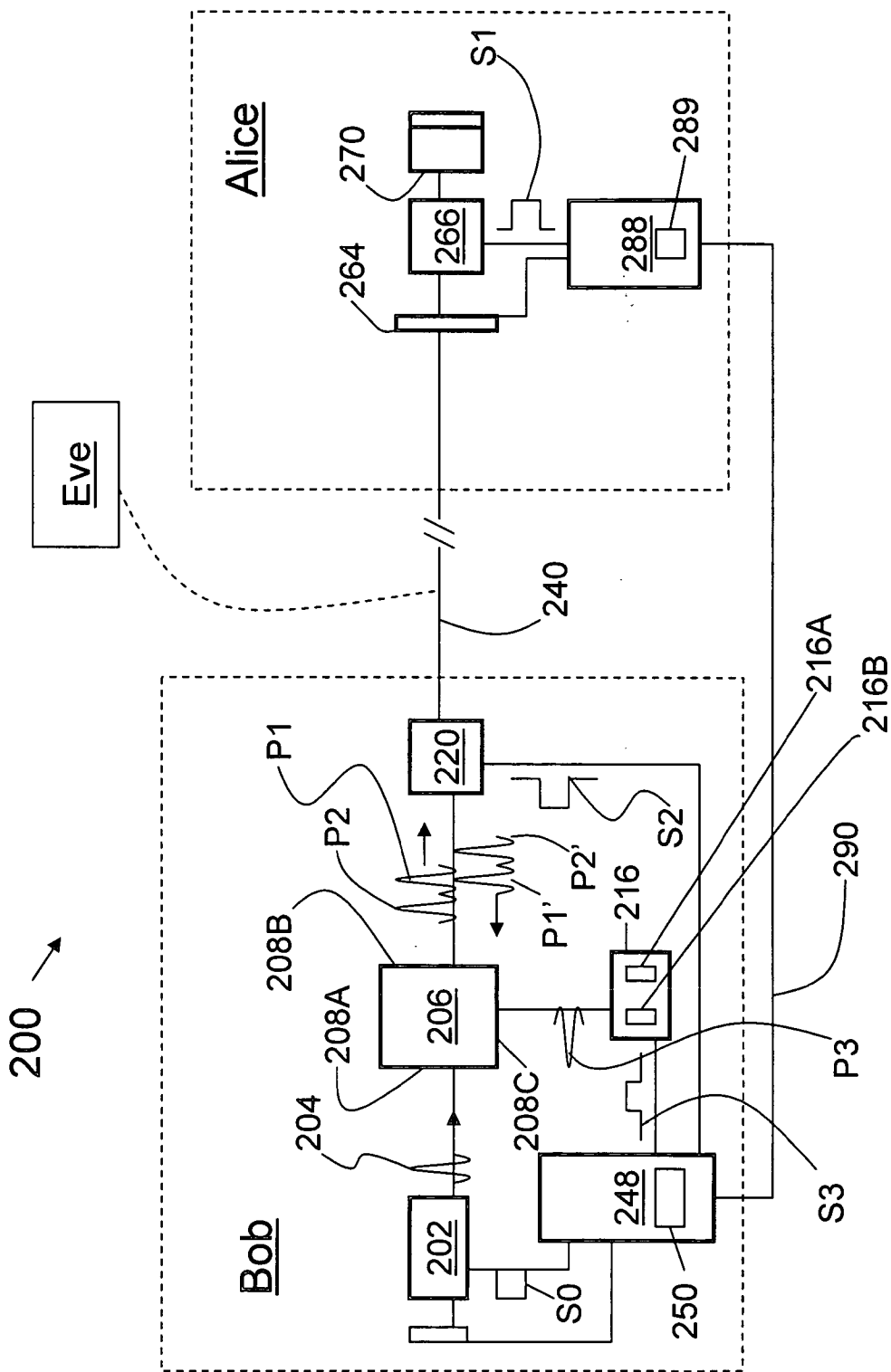


FIG. 1

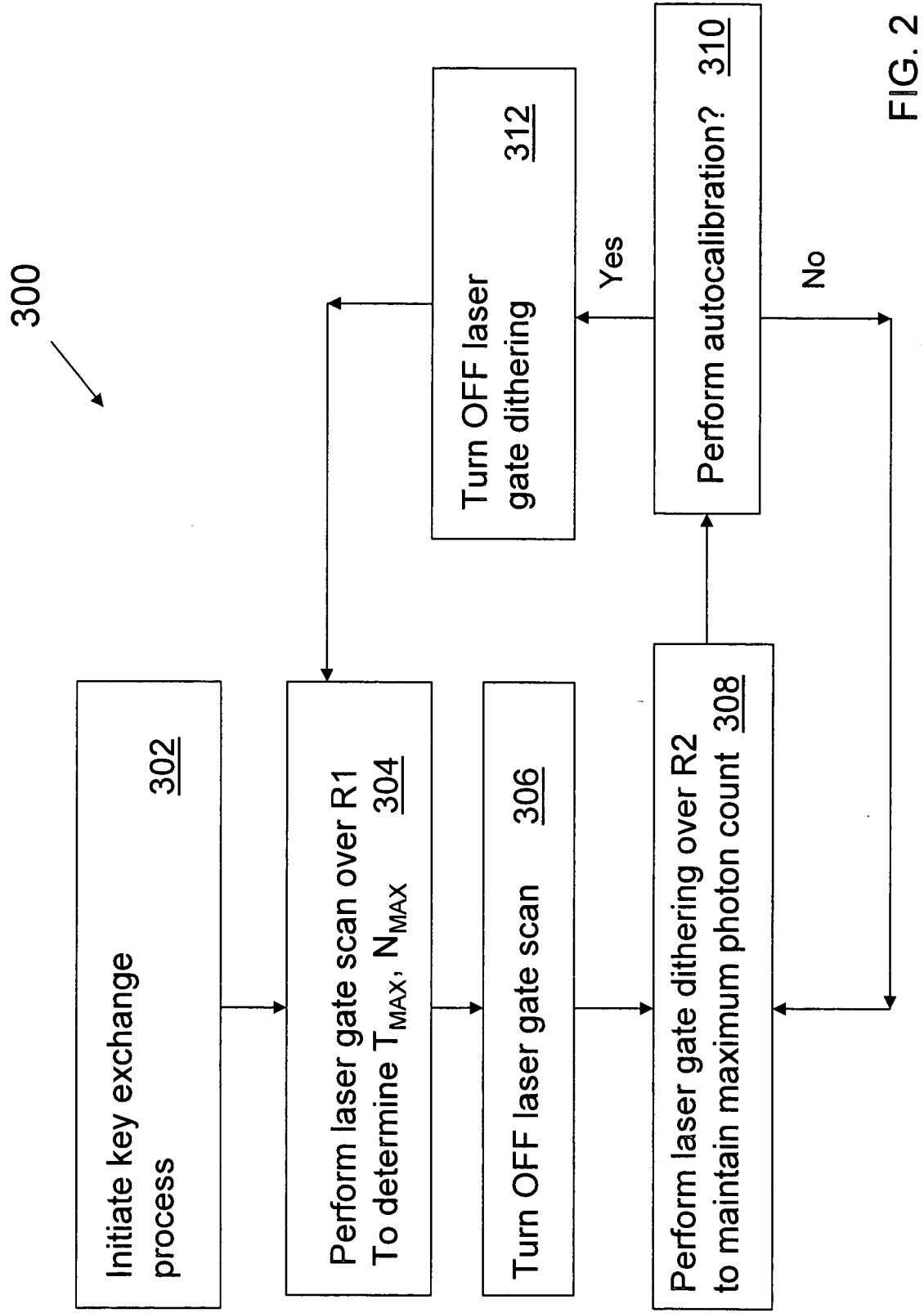


FIG. 2

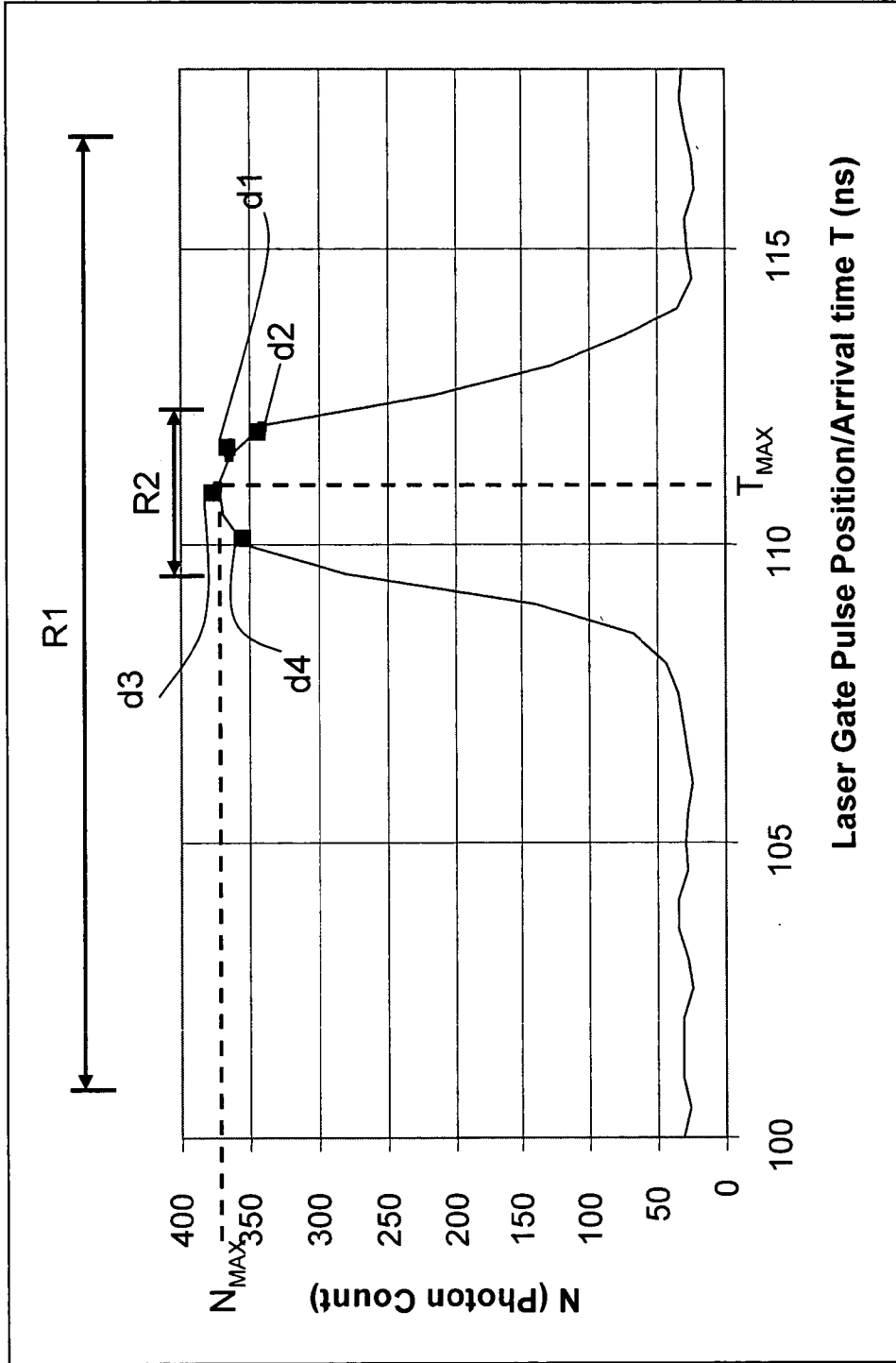


FIG. 3